International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 4, Issue 2, Apr 2014, 151- 158

TRANS STELLAR
• Journal Publications • Research Consultancy

COMPARATIVE ANALYSIS OF TRUST BASED AND INTRUSION BASED BLACK HOLE PREVENTION IN AODV IN MANET

RAJSHEKHAR TIWARI & MANISH SHARMA

Department of Electronics & Communication Engineering, Sanghvi Institute of Management & Science, Indore, Madhya Pradesh, India

ABSTRACT

The Black hole attack is a serious threat in a mobile ad-hoc network (MANET). It has shown that blackhole effect can be minimized through adding trust agent in routing protocol as well as applying intrusion detection techniques. Here a performance Comparison is carried out between modified AODV trusted environment and modified AODV with specification based intrusion detection system. Various QOS parameter like throughput, NRL and Packet Delivery Fraction using open source simulation tool NS2 has been analyzed.

KEYWORDS: Ad-hoc, Trust with Delay Calculation, Routing, IDS

1. INTRODUCTION

Ad hoc networks are limited capacity networks with no network infrastructure and no dedicated routing devices. Moreover, every node in such networks has to take care of its routing module itself. The main advantage of wireless network is communicating with rest of the world while being mobile. A Mobile Ad-hoc Network (MANET) is a collection of independent mobile users that communicate with available bandwidth and limited power. As the nodes in a MANET are mobile, the network topology may change rapidly [1]. The most important characterizing feature of a MANET is that no one among all has the central role. So there is a big scope of secure algorithm which can serve the best in this mobile scenario. The Black hole attack is a serious threat in a mobile ad-hoc network (MANET). In this attack a, malicious node injects a faked route relay message to deceive the source node so that the source node establishes a route to the malicious node and sends all the data packets to the malicious node [2]. There are also various attacks in ad hoc wireless network, mainly divided in five categories-Impersonation, Modification, Fabrication, Replay and Denial of Service (DoS). Black hole attack belongs to category of fabrication attacks. Obviously this black hole attack degrades the Quality of Service in terms of packet dropping. There are several techniques proposed by the researchers to handle this problem. Trust based routing and Intrusion detection systems are widely accepted techniques. Here AODV protocol with trust with delay calculation and AODV with specification based intrusion system are used to analyze blackhole effect in both. The rest of the paper is organized as follows- section 2 describes related works and section 3 proposed works .Result and analysis are presented in section 4 followed by conclusion in section 5.

2. RELATED WORKS

The selection of more trusted route becomes an important aspect of Ad-hoc network. To provide a trust based routing protocol several trust evaluation models are proposed by various researchers. Jain, Jain and Sagar proposed Trusted AODV (TAODV) [3] where the nodes assist and trust each other in forwarding packets from one node to another to get a

more trusted path. But it suffers from some assumptions, which a node may need to recover from its neighbor node. R. S. Mangrulkar, Pallavi V Chavan, S. N. Dagadkar proposed a model called Trust Based AODV [4] initially a trust value 100 is set to all the nodes in the network. Then after transferring a packet from one node to another node this trust value is increased to 200. In this method a higher trust value is assigned when a node forward a packet. And this method is not so strong to detect a black hole node and to exclude it from its route. The related work roughly may be categorized into two sub-areas: authentication-based approaches erected at the ad-hoc routing protocols, and general IDS targeted at mobile ad hoc networks. The primary work in securing routing protocols has addressed the problem of implementing effective integrity mechanisms. Approaches that impose authentication and integrity mechanisms are found in ARAN [5] [6] and S-AODV [7] among others. The latter also includes a useful description of exploits in the ad hoc domain.

In this paper the trust value of a node is calculated depending upon the packet forwarding ability and a weight factor. This weight factor is defined as the ratio of number of RREP set to the number of RREQ received by the node. This trust value along with threshold delay is inserted in the routing table and the route discovery is done according to this trust value by avoiding a node which has lesser trust value and threshold delay.

3. PROPOSED WORK

In this paper considers two proposed protocol extensions to secure MANET routing. In the first trust with delay calculation TWDCBAODV [8], a rank is generated based on this trust value. This trust value is calculated depending upon the ability to forward packets and the RREQ forwarding ability of a node. To obtain this ability the number of packets received and the number of packet sent is counted. Two weight factors W1 and W2 are introduced. W1 is the ratio of number of packets sent from a node to the number of packets received to that node. A high value of this ratio indicates that, the node has a greater ability to forward the packets. Thus the probability of loss of packets is less. The maximum value of W1 may be 1, where all the received packets are forwarded and no packet is dropped. From this value we can also detect suspicious nodes in the network. The other weight vector W2 is the ratio of number of RREQ received to number of RREP sent. This ratio detects the nodes which continuously receive the RREQ from its neighbor nodes but never respond to that request by sending the reply i.e. the silent node. Thus the higher value of this ratio means that, the nodes can frequently respond to the route request of its neighbor node. Then this two weight factor is multiplied to get the trust value of that node. Here we check if any nodes have the W1 value greater than the threshold value. If it can send a packet then the trust value is increased otherwise it is decreased. This trust value is saved in the routing table of that node. And in the route discovery step of AODV routing protocol the path is established according to that trust value rather than the shortest path. Thus the less trusted node can be avoided during the route establishment in AODV routing protocol.

At the same time a delay threshold generated. In the route discovery step of the AODV routing protocol a path is chosen in such a way that more trusted nodes with delay threshold are involved. Also a node can be excluded which is either not trusted or having below delay threshold value, from the route. Thus the packet is transferred through a more trusted path rather than the shortest path.

The second, specification based SBIDSAODV [9], defines a set of constraints that explains the correct operation of a program or protocol. It checks the execution of the program with respect to defined constraints. This technique provides a capability of detecting previously unknown attacks with low false positive rate.

3.1. Trust Calculation

The original TRUSTAODV uses a very simple model, with each node associated to an integer trust value initialized to 0. That value is simply incremented for nodes that are detected to forward packets and decremented for nodes that do not appear to forward the packet.

```
void TrustNode::increaseTrust()
{
        trustValue++;
}
void TrustNode::decreaseTrust()
{
        trustValue--;
}
```

Malicious and faulty nodes are then bared from the network once they obtain a score of -10.

```
bool TrustNode::isNodeTrusted()
{
        if(trustValue <= -10)
        {
                return false;
        }
        else
        {
                return true;
        }
}
```

3.2. Delay Calculation

Apart from to find better trust value for a particular node we added a new agent Delay. Now the generated route depend upon the higher trust value and delay more than or equal to threshold delay.

Steps

- Find the minimum time (t_{min}) taken by two far most nodes in control packets transmission.
- Set this time as threshold delay.

- Any packet which one pretended to deliver packets in time lesser than threshold delay time may be a malicious node.
- This node must be avoided in route path.

A Sample Code from twdcaodv.cc File for Delay Agent is as following-

```
if(delay > 0.0) {
    Scheduler::instance().schedule(target_, p, delay);
  }
else {
  // packet sends immediately
    Scheduler::instance().schedule(target_, p, 0.);
else if(tsv<0.3){
rt->rt_trv=tr_trv+1;
if(rt->rt_trv<4)
rt->rt_trv
nb_delete(iht);
```

// Not a broadcast packet, lesser than t_{min} delay, avoid immediately.

3.3. Simulation Environment

The NS2 simulation software is used to simulate the proposed approach. NS2 is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators. Network is meant in a broader sense that includes wired and wireless communication networks, on-chip networks, queuing networks, and so on. Domain-specific functionality such as support for sensor networks, wireless ad-hoc networks, Internet protocols, performance modeling, photonic networks, etc., is provided by model frameworks, developed as independent projects. NS2 is a discrete event simulation environment.

3.4. Simulation Parameter

For simulation of the above proposed approach/technique we consider the following parameter values of the network and use the AODV routing protocol.

Table 1: Parameter Value for Simulation

Parameter	Value
Routing protocol	AODV
No of node	20
Node separation	150
Node mobility type	mass
Mobility speed	50mbps
Traffic type	CBR

The snap shot of the simulation information is shown in the figures given below.

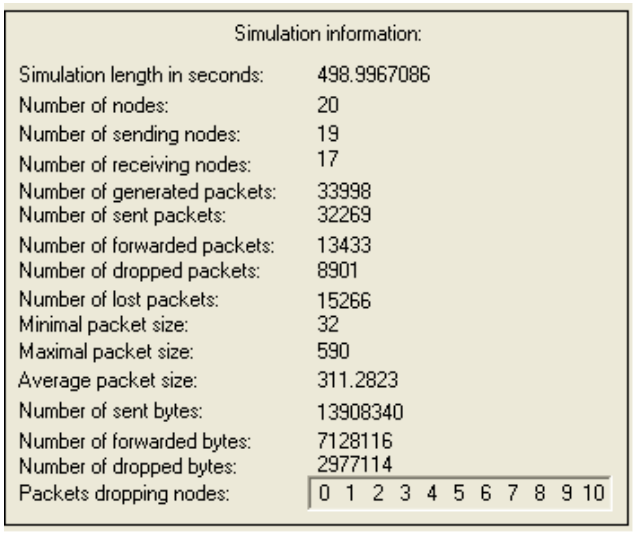

Figure 1: Simulation Information for AODV Trust with Delay Calculation

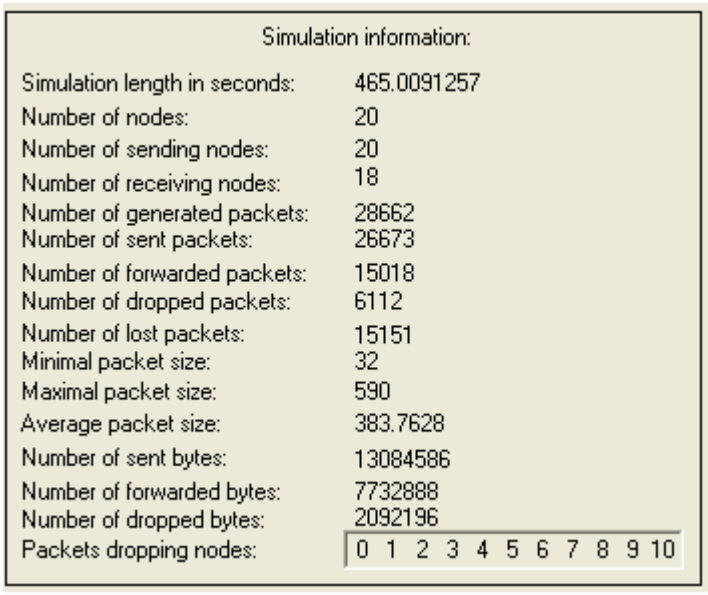

Figure 2: Simulation Information for Specification Based IDSAODV

4. RESULTS AND ANALYSIS

Performance Metrics are quantitative measures that can be used to evaluate any MANET routing protocol. The metrics that compare the performance of normal TWDCAODV and SBIDSAODV under blackhole attack are as follows:

- **Throughput:** The total bytes received by the destination node per second (Data packets and Overhead).
- **Total No of Packets Dropped:** Number of packets dropped (i.e. send-receive) due to random traffic generation or due to abnormal behavior of AODV.
- **Packet Delivery Fraction (PDF):** The ratio of the data packets delivered to the destinations to those generated by the sources.

- **End 2 End Delay (e2e):** Time consumed between sending node and receiving node.

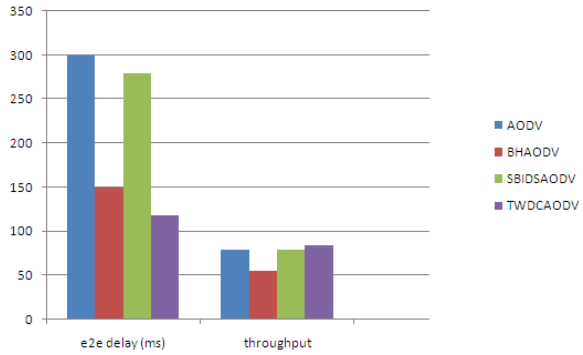

Figure 3: Other QOS Parameters Comparison the Graph Shows that TWDCAODV has Minimum End to End Delay and Maximum Throughput

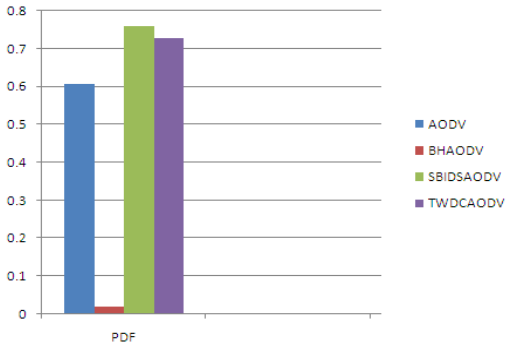

Figure 4: PDF Comparison

Figure 4 Shows that TWDCAODV has Lesser Packet Delivery Fraction as Compared to SBIDSAODV

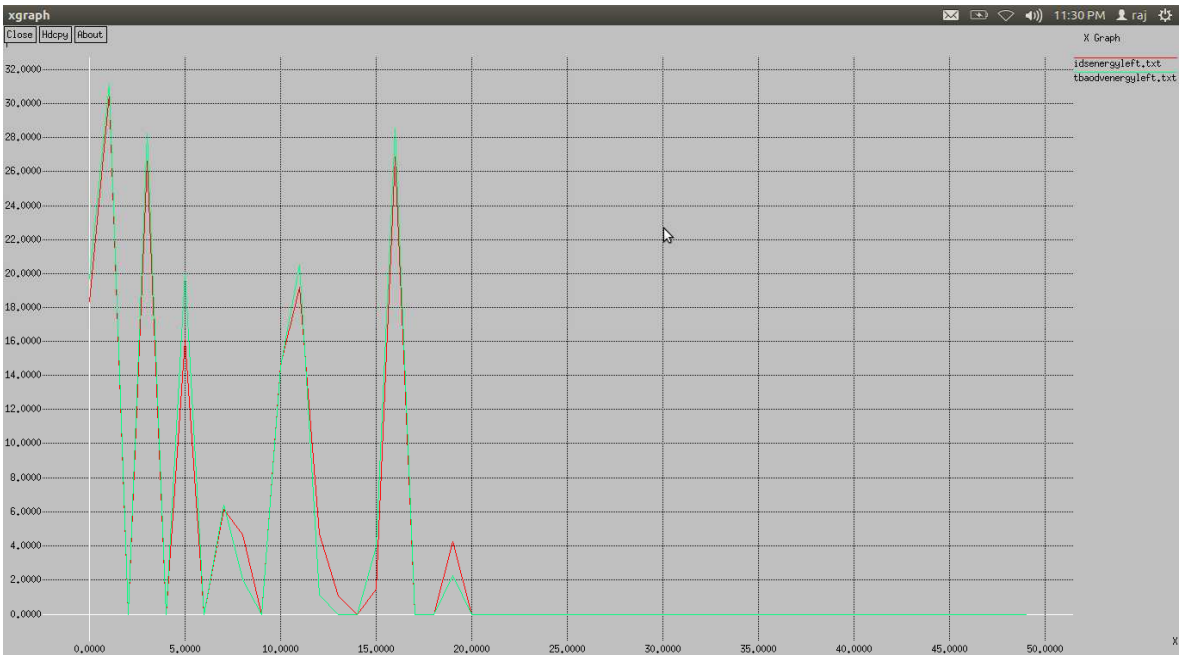

Figure 5: Energy Comparison

Figure 5 Shows that Trusted Protocol has Better Energy Efficiency as Compared to IDSAODV

5. CONCLUSIONS

MANET is at the center of wireless technology. Due to lack of infrastructure there are lot of security threats. Black hole is one of them, where certain node swallows all the packets in the network no packet is forwarded towards its original destination. Therefore the quality of service of the network becomes an important issue with respect to packet dropping. Here a analysis had been done through simulation using highly reliable tool like Network Simulator (NS2). Here we gives summarize result in normal AODV protocol case, Black Hole Attack case, Trusted AODV and IDSAODV case. It is clear that trusted environment has better performance as compared to IDS system. Here a trust value is calculated to each node. A threshold delay is also calculated. Depending upon the trust value and the threshold value the black hole node is identified and it is excluded from the route establishment process. Thus the packet is transferred through a more trusted path rather than the shortest path. As its avoided low trusted path, the packet loss is also decreases and the quality of service of the network is enhanced in terms of packet loss.

REFERENCES

1. Radha Krishna Bar, Jyotsna Kumar Mandal and Moirangthem Marjit Singh, “QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack”, International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.
2. Ankit Jain, Arnika Jain and Pramod Kumar Sagar Journal of Global Research in Computer Science 32-36 Vol.10 Issue 14 (Ver.1.0) November 2010.
3. R. S. Mangrulkar, Pallavi V Chavan, S. N. Dagadkar, “Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT”, International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010.
4. A.Menaka Pushpa M.E., “Trust Based Secure Routing in AODV Routing Protocol” (2009).
5. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks”, In Proceedings of the Eighth ACM Intl. Conf. on Mobile Computing and Networking (MobiCom’02), ACM, Atlanta, Sept. 2002, pp 12-23.
6. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields and E. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks”, In Proceedings of IEEE ICNP, 2002.
7. L. Zhou and Z. J. Haas, “Securing ad hoc networks”, In IEEE Networks, 13(6):24-30, 1999.
8. R. S. Mangrulkar, Pallavi V Chavan, S. N. Dagadkar, “Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT”, International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010.
9. Yibeltal Fantahum Alem & Zhao Hheng Xaun, “Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection”, Tainjin 300222, China 2010.